Book reviews

Yearning for the impossible: The surprising truths of mathematics

John Stillwell
A. K. Peters, Ltd., 2006, ISBN 156881254X

In a nutshell: This is a great book, read it!

Many readers of the *Gazette* will be familiar with the beautiful books by author John Stillwell, such as ‘Mathematics and its History’, ‘Geometry of Surfaces’ and ‘Classical Topology and Combinatorial Group Theory’. Unlike the texts that John Stillwell is famous for among mathematicians, ‘Yearning for the Impossible’ is aimed at a general audience. However, this does not mean that it is filled with trivialities, or is devoid of real mathematics, as is true for many popularisations of mathematics. On the contrary, realising that there is still ‘no royal road to mathematics’, the author’s aim is to strike just the right balance between mathematical content and conveying the beauty of mathematics. He achieves this by writing so that ‘readers with a good mathematical background from high school should be able to appreciate all, and understand most, of the ideas in the book’. In this he succeeds brilliantly, and, furthermore, I cannot imagine anybody with a more sophisticated background in mathematics not also enjoying this book.

In the preface of his book Stillwell writes:

> There are many instances of apparent impossibilities that are important to mathematics, … Mathematical language is littered with pejorative and mystical terms — such as irrational, imaginary, surd, transcendental — that were once used to ridicule supposedly impossible objects. And these are just terms applied to numbers. Geometry also has many concepts that seem impossible to most people, such as the fourth dimension, finite universes, and curved space — yet geometers (and physicists) cannot do without them … Mathematics is a story of close encounters with the impossible because *all its great discoveries are close to the impossible.* The aim of this book is to tell the story, briefly and with few prerequisites, by presenting some representative encounters across the breadth of mathematics.

The different chapters of the book are entitled: ‘The Irrational’; ‘The Imaginary’; ‘The Horizon’ (projective geometry); ‘The Infinitesimal’; ‘Curved Space’; ‘The Fourth Dimension’; ‘The Ideal’ (numbers beyond numbers); ‘Periodic Space’ (Escher worlds in mathematics); and ‘The Infinite’. Looking at these titles many readers of the *Gazette* will think: ‘Been there, done that, know everything there is to know and can be said to a lay person about these things’. While it is true that many of the topics listed here have been written about by many other popularisers of mathematics, John Stillwell manages to find many, many new and interesting angles to keep even experts entertained.

Here are just a few details to whet your appetite. ‘The Irrational’ is a beautiful exposition of the basics of irrational numbers, which includes the Pythagorean theory of musical harmonies based on rational numbers, the problems this theory encounters (the Pythagorean comma), and how these problems are naturally overcome by introducing the equal temperament which is based on the irrational frequency ratio of $\sqrt[12]{2}$. This chapter also includes some of the gems produced by the theory of continued fractions, a beautiful topic which seems largely forgotten. The chapter ‘Curved Space’ starts out as follows:

> People of ancient and medieval times are often said to have believed that the earth was flat, a belief supposedly overthrown by Christopher Columbus. This is a myth. *Not only did the ancients know that the earth was round, they believed that space was round too — an idea that seems impossible to most people today.*

Sound interesting? What do you expect to read about in a chapter entitled ‘The Fourth Dimension’? Quaternions?

The book itself, a hardcover edition, is very well produced and is a pleasure to browse around in. Most pairs of facing pages contain at least one graphical element; unlike most mathematical textbooks, the original illustrations were done by someone who knows what they are doing; and the layout is open and uncluttered.

To summarise: This is a great book, read it!

Burkard Polster
Department of Mathematics and Statistics, PO Box 28M, Monash University, VIC 3800.
E-mail: Burkard.Polster@sci.monash.edu.au

◇ ◇ ◇ ◇ ◇ ◇

Applications of abstract algebra with Maple and Matlab 2nd edition

Richard E. Klima, Neil P. Sigmon and Ernest L. Stitzinger
CRC Press, 2006, ISBN 978-1-5848-8610-5

There is much to admire and like about this book. Its robust and expert use of Maple and Matlab — the leading software for symbolic and numerical work respectively, the breadth of material covered, and the generous exercises all mark it out as deserving high praise.

That being said, I have a few caveats with this book. First, it is not a standard mathematics text, where a theory is carefully built up with axioms, lemmas, propositions, theorems and corollaries, all with proofs, but rather a book which shows how Maple and Matlab can be used to elucidate and illustrate algebraic material. Second, possibly because of the first point, a somewhat cavalier attitude has been taken to some of the topics: there are places in the book where more explanation and a greater attention to detail would have been appropriate. For this reason the book is unlikely to be used as a text in a standard course, but rather as an adjunct to a course in modern applications of algebra.

I will enlarge on these points below.

Material covered

The authors cover a brave range of material: block designs and difference sets; error-correcting codes — including Hamming codes, Reed–Muller Codes, BCH codes and Reed–Solomon codes; classical cryptography — shift, affine, Vigenère and Hill ciphers; RSA and ElGamal cryptosystems; elliptic curves and elliptic curve cryptosystems; the Advanced Encryption Standard; Burnside's theorem and Pólya's counting theorem; graph theory and graph counting.

Chapter 1 discusses 'Preliminary Mathematics'; mainly groups, rings and finite fields and the implementations of finite fields in Maple and Matlab. The material here is standard, and treated briskly, but with due care. Curiously, there is no mention of the fundamental fact that any two fields of order p^n are isomorphic. The treatment of fields in Maple relies on constructing powers (modulo the defining polynomial) of a primitive element. This certainly is how one might generate a small field by hand, but surely it would be both more standard and lead to greater power if the authors used Maple's own finite field package `GF`.

Chapter 2 investigates block designs, Hadamard matrices and difference sets. Some fundamental results are given (but not the Bruck–Ryser–Chowla theorem). I think the authors missed an opportunity here to include some material on finite projective planes.

Chapters 3, 4 and 5 present some elementary material from the theory of error-correcting codes. Specifically: linear codes, Hamming and BCH codes, Hadamard codes, Reed–Muller and Reed–Solomon codes. Although perfect codes are mentioned, the Golay codes are not. The authors provide only the decoding of Reed–Muller codes using Hadamard matrices; majority logic decoding is not mentioned. In the sections on basic linear codes, Hamming codes and Reed–Muller codes, Matlab is used appropriately; its matrix handling used efficiently and well. For the BCH and Reed–Solomon codes, whose definition requires some symbolic algebra, the best the authors can do with Matlab is to call Maple commands from within it. I wonder if it might simply have been better to admit that here Matlab is the wrong tool for the job. In fact of course Reed–Solomon codes can be implemented very efficiently in Matlab, but not in the way that the authors have described them. This is one of the problems faced by using both Maple and Matlab — the intersection of problems efficiently solvable by both is quite small.

In Chapter 6 we move into 'Algebraic Cryptography': shift and affine ciphers, and the Hill matrix cryptosystem. The mathematics here is simple, but entertaining, and both Maple and Matlab are appropriately used. Chapter 7 is entirely devoted to the Vigenère cipher and its cryptanalysis with the index of coincidence. I think that an entire chapter devoted to the Vigenère cipher is too much. This cipher is cryptographically trivial, and although some discussion of its cryptanalysis is necessary, I would rather more time be spent on modern cryptosystems. In particular, the RSA and ElGamal cryptosystems are presented purely as algebraic constructs.

Chapter 7 discusses the RSA cryptosystem and the Diffie–Hellman key exchange — both vital topics in modern cryptography. Here Maple is used entertainingly to illustrate RSA, using commands which transfer a string of upper case characters to and from a large integer, by treating each letter's place in the alphabet as a 'digit' in base 100. As with many chapters in the text, this is a place where Matlab is unsuited for the task, and most of the Matlab commands in this chapter are calls to the Maple kernel. This chapter also contains 'Notes' on integer factorisation, primality testing, digital signatures and modular exponentiation. With the exception of the last, all these topics could have benefited from greater detail. Space would have been better used in this book by eliminating Matlab and enlarging these important topics.

Elliptic curves and associated cryptosystems are the topic of Chapter 8 — a change from the first edition of this book, where elliptic curves were only part of a chapter. A starting point is the ElGamal cryptosystem, but the authors miss out on the opportunity to introduce primitive roots. They do not in fact spend any time discussing the base a in

$$a^n \pmod{p}$$

where $n < p$ is randomly chosen. To their credit, the system is first introduced over general Abelian groups, but even so too much detail is omitted. Elliptic curves are first introduced in the Cartesian plane and the standard geometric construction is given for point addition and doubling. Then the construction is given algebraically in terms of the point coordinates. This is all very well, but surely a few lines explaining how the point addition formulas are derived from the geometric construction could have been included. Also, a brief nod in the direction of elliptic functions as a basis for the entire theory would have been appropriate. If Pollard's $p-1$ method had been introduced in the previous chapter, this would have been an excellent place for Lenstra's elliptic curve factorisation method.

Chapter 10 is devoted to the Advanced Encryption Standard; the Rijndael cryptosystem. The trouble here is that because of the authors' clumsy implementation of finite fields, much of the advantages of using Maple to illustrate the AES are lost. It may have been better to describe the AES, but use Maple (or Matlab) to illustrate a simpler version, possibly that of Musa *et al.* [1].

One major oversight in all of Chapters 8–10 is that no discussion of weaknesses of any of these cryptosystems is given. There is no discussion about their security, attacks against these systems, and how such attacks can be subverted. This is disingenuous, as it gives the impression that the security is based only on the difficulty of factoring or of discrete logarithms, and not on how they are used.

Chapter 11 considers enumeration; specifically Burnside's theorem and Pólya's enumeration theorem. This chapter is really well done; with excellent examples and a careful and considered approach to the subject. In the book's introduction, the authors state '... we should also note that Chapter 11 has always been one of our and our students' favorites'. I would agree in the sense that this is one of the best chapters in the book, from the point of view of the excellence of its mathematics, and of the use of software. Chapter 12 continues this subject and provides an example of the use of enumeration techniques to graph counting.

Exercises

An otherwise excellent textbook can fall on the basis of poorly written exercises. I am pleased to report that this is not the case here — the authors are clearly meticulous in their teaching, and the exercises all through the book are models of their kind. Each chapter finishes with three groups of exercises, headed 'Exercises', ‘Computer Exercises’ and ‘Research Exercises’. The last are invitations for the student to explore the history and uses of the chapter’s material.

Software used

The authors have chosen Maple and Matlab. In the first edition of this book, Maple alone was used. I expect that the authors decided to include Matlab because it is the most popular numerical software currently available. However, much of the material in this book is concerned with algebraic manipulation, or arithmetic on arbitrarily large integers — both are topics not handled by Matlab! This means that much of the Matlab code samples are simply commands which call Maple code, using a Maple kernel embedded within Matlab. For example, the Maple command given for computing a discrete logarithm is given as

```
> mlog(1438, 256, 8383);
```

and the corresponding Matlab code is

```
>> maple('mlog', sym('1438'), sym('256'), sym('8383'))
```

I think the authors would have been better to use Mathematica instead of Matlab, or indeed any other system which allows for algebraic manipulation and large integer arithmetic. And I would expect that most academics or students who would acquire a book such as this would have access to at least one of Maple or Mathematica.

I find it odd that there is a great amount of finite fields in the book, but no mention of Maple’s GF package for computations on finite fields. Admittedly, it’s a clumsy implementation, but as it’s standard Maple I think the authors should either have used it, or explained why they decided not to.

Some of the code is unnecessarily clumsy and obtuse. For example, the authors take seven lines of Maple code to provide a method which will convert letters of the alphabet to the integer values 0 to 25:

```
>  letters := array(0..25, ["A", "B", "C", "D", "E", "F",
>  "G", "H", "I", "J", "K", "L", "M", "N", "O", "P", "Q",
>  "R", "S", "T", "U", "V", "W", "X", "Y", "Z"]):
>  ltable := table():
>  for i from 0 to 25 do
>      ltable[ letters[i] ] := i;
>  od
```

Since these particular lines of code occur in three separate places in the book, I assume that the authors believe that this is the best way of establishing a correspondence between letters and numbers. These tables and arrays are then used as follows:

```
>  message := "ATTACK AT DAWN";
>  message := Select(IsAlpha,message);
>  ptext := convert(message,list);
>  ptext := map(i -> ltable[i], ptext);
```

However, all of this can be done simply in two lines with Maple's `convert,bytes` mechanism, and a shift of 65:

```
> ptext := "ATTACKATDAWN";
> map(x->x-65,convert(ptext,bytes));
```

Why didn't the authors choose this vastly simpler method? Shorter code is usually best, if it is not unnecessarily obfuscated. It seems as though the authors have not really updated their code since the first edition of the book, to take advantage of the strengths and increased functionality of newer versions of Maple.

Final remarks

I would probably not use this book as a basis for a course myself, but I do like it as a reference, and as an example of the use of modern software to illustrate mathematics. In terms of the material covered and use of software, I prefer the approach of Trappe and Washington [2].

The use of Matlab, as I have said earlier, is not really suitable for an algebra text. Matlab's strengths are in numerics, not algebra.

However, this text shows a lovely interplay between mathematics and software, and it is the sort of text of which I hope to see much more.

References

[1] Musa, M., Schaefer, E. and Wedig S. (2003) A simplified AES algorithm and its linear and differential cryptanalyses. *Cryptologia* **27,** 148–177.

[2] Trappe, W. and Washington, L. C. (2005). *Introduction to Cryptography with Coding Theory*, 2nd edn. Prentice-Hall.

Alasdair McAndrew
School of Computer Science and Mathematics, Victoria University, PO Box 14428,
Melbourne 8001, VIC. E-mail: Alasdair.McAndrew@vu.edu.au